

**Amendments to the Specification:**

*Please replace the paragraph beginning on page 3, line 27, with the following amended paragraph:*

Referring next to Fig. 2, a block diagram of another embodiment of a CA system 200 is illustrated. This embodiment 200 shows the functional blocks 204, 208, 212 that receive the content and distribute it to the set top boxes 108. These functional blocks 204, 208, 212 could reside in the ~~headed~~ headend 104. Included in the CA system 200 are a permissions, resource, object signatory (PROS) software 204; a message spooler 208; an object spooler 212; a distribution network 216; and a number of set top boxes 108.

*Please replace the paragraph beginning on page 7, line 21, with the following amended paragraph:*

Referring next to Fig. 6, an embodiment of a "rights" message 600 is shown in block diagram form. The rights message 600 conveys rights to use a functional unit. The functional unit could be an object or a resource. Typically, there is one rights message 600 for each set top box 108, which specifies any rights for all functional units. Requirements from the authorization message 300 that are associated with objects and resources are checked against the rights to determine if interaction with ~~another object~~ another object or resource is authorized. The rights message 600 allows remotely adding new rights to a functional unit associated with the set top box 108. Although not shown, the rights message 600 typically includes a digital signature to verify the integrity of the message 600 during transport. In some embodiments, a checksum could be used instead of a digital signature.

*Please replace the paragraph beginning on page 8, line 23, with the following amended paragraph:*

Superordinate functional units are designed to initiate execution of the checkpoints and subordinate objects are designed to have checkpoints imposed upon them. For example, the BIOS 708 requires execution of a checkpoint upon the OS 712 during the boot process, during execution and/or periodically while running. A driver object 718 is subject to

checkpoints when installed or exercised during normal operation. Data file objects 722 are subject to checkpoints whenever the data in the file is accessed. An HTML object 728 is reviewed as part of a checkpoint whenever the HTML object 728 is interpreted by a browser application 716. **JAVA™ applications 724 are in a stratum above a JAVA™ virtual machine 720. Resources 714 are in the same stratum as the JAVA™ virtual machine 720.**

*Please replace the paragraph beginning on page 8, line 31, with the following amended paragraph:*

Referring next to Fig. 8, interaction between functional units is shown in block diagram form. The functional units associated with the set top box 108 include a set top box resource 804, a printer driver object 808, an e-mail object 812, and a printer port resource ~~816~~ **814**. During the normal interaction of these functional units, checkpoints are encountered that trigger authorization and/or authorization checks. The sole table correlates rights and requirements to each functional unit in Fig. 8. The functional unit identifier serves to correlate the software messages 400 with their authorization messages 300.

*Please replace the paragraph beginning on page 10, line 4, with the following amended paragraph:*

Once the signature 312 is calculated, the authorization, software and rights messages 300, 400, 600 are created in step 916. At this point, the messages 300, 400, 600 are complete except for the checksums 316, 412, 612. In step 920, the authorization, software and rights messages 300, 400, 600 are sent to the message and object spoolers 208, 212. Only the set top boxes 108 that will be authorized to use the software object 408 require replacement rights messages 600. Once the spoolers 208, 212 receive the authorization, software and rights messages 300, 400, 600, the checksums 316, 412, 612 are calculated **in step 924** to complete all fields in the messages 300, 400, 600.

*Please replace the paragraph beginning on page 10, line 12, with the following amended paragraph:*

After the authorization, software and rights messages 300, 400, 600 are complete, they are separately sent to the set top boxes 108. In step 928, the authorization message 300 is broadcast to the set top boxes 108 over a network 216. The network 216 could include a control data channel, MPEG data stream and/or packet switched network. After the authorization message 300 is sent, the rights message 600 is singlecasted to each affected set top box 108 in step 930. Once the authorization and rights messages 300, 600 are received **after broadcast in step 932**, the set top box 108 can determine authorization. .

*Please replace the paragraph beginning on page 11, line 20, with the following amended paragraph:*

If the calculated and received signatures match, as determined in step 1036, the software object 408 is authenticated as originating from an approved source and has not changed since being signed. Authenticated software objects 408 are retained and used by the set top box in step 1040. If the software object fails authentication in step 1036, the software message 400 is discarded and an error is reported back to the headend 104 **in step 1044**. By using this process, software objects are verified, authorized and authenticated before use.